



SPYWOLF

Security Audit Report



Completed on
August 25, 2022

MADE IN USA 

 @SPYWOLFNETWORK

 @SPYWOLFNETWORK

 SPYWOLF.CO



OVERVIEW

This audit has been prepared for **Procyon** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

The following contracts which are part of the project are out from the scope of current audit:

PCYPresale contract - 0x7FCBD0B62c73bE8224785af793813b3De3AE1Cf8

ProcyonFund contract - 0xa37cC1fB0f53dcf164b3ec19a61E971d42a49809

ProcyonFarmingReferral contract - 0x464071a38D23de96E02aAc9055Ae9cBE0013F6Bf

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”

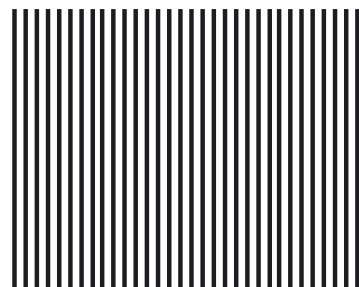




TABLE OF CONTENTS

Project Description	01
Contract Information	02
Contract 1 Stats	02-07
Contract 2 Stats	08-14
Contract 3 Stats	15-16
Contract 4 Stats	17-18
Good Practices	19
Tokenomics	20
Team Information	21
Website Analysis	22
Social Media & Online Presence	23
About SPYWOLF	24
Disclaimer	25



Procyon



PROJECT DESCRIPTION

According to their whitepaper:

Procyon Finance is a Decentralized Algorithmic Exchange market that allows participants to engage in the well-established protocol. Users who provide liquidity for the market earn passive income from many capital-efficient financial features, while traders can trade in an open-integrated market, enabling peer-to-peer transactions in the most stable platform on the DeFi market.

Release Date: Presale starts on August, 2022

Category: DEX



CONTRACT 1 INFO

Token Name PCY Token	Symbol PCY
Contract Address 0xAd421C4F5F091f597361080d47B6f44ED44F155a	
Network Cronos Chain	Language Solidity
Deployment Date August 22, 2022	Verified? Yes
Total Supply 1,000,000	Status Not launched

TAXES



*Taxes cannot be changed



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of August 25, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
No limit

DEX:
Procyon

LP Address(es)

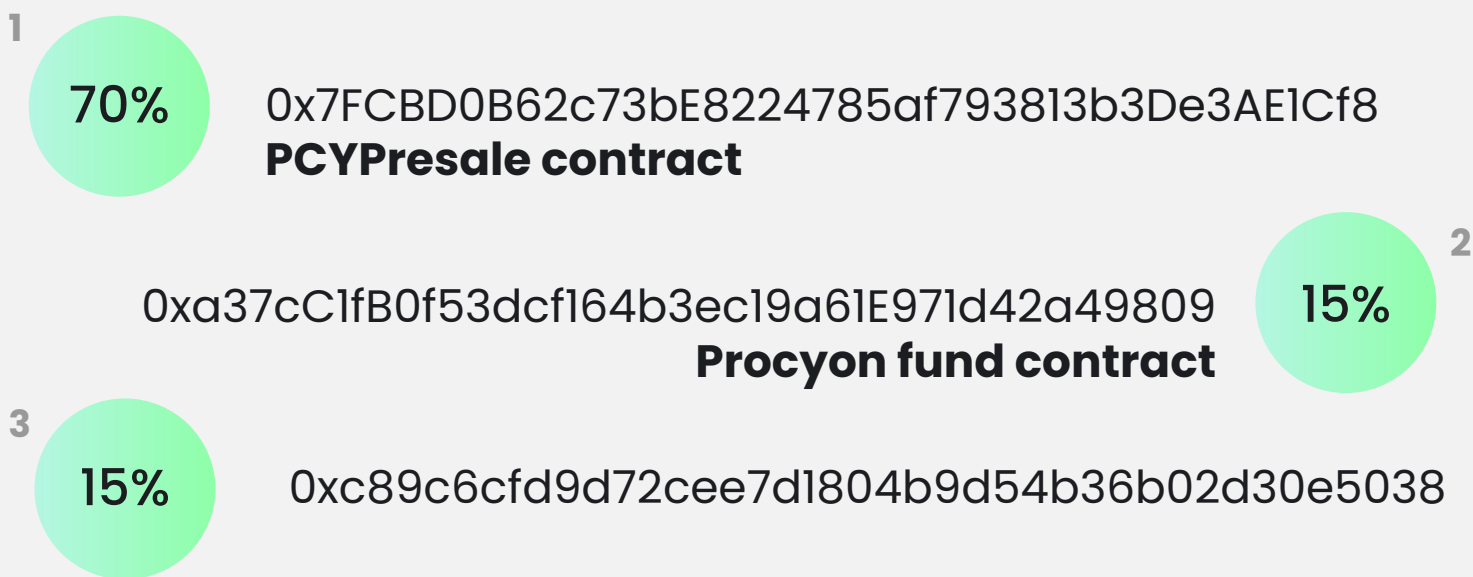
Liquidity not added yet



FEATURED WALLETS

Owner address	0x27e85f98b48d447d0148afeca7b149b0e69c2c2e
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can mint (create) new tokens.
This can lead to token's price inflation.

```
function mint(uint256 amount) public onlyOwner returns (bool) {  
    _mint(msgSender(), amount);  
    return true;  
}  
  
function mint(address _to, uint256 _amount) public onlyOwner {  
    _mint(_to, _amount);  
    _moveDelegates(address(0), _delegates[_to], _amount);  
}
```

CONTRACT 2 INFO

Token Name	Symbol
ProcyonFarming	N/A
Contract Address	
0x27e85F98B48D447D0148AFeCa7b149b0E69c2c2e	
Network	Language
Cronos Chain	Solidity
Deployment Date	Verified?
August 22, 2022	Yes
Total Supply	Status
N/A (Farming contract)	Deployed

TAXES



*Taxes can be changed for each pool in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



FEATURED ADDRESSES

Owner address	0x06d8dfb08f3d87cf2d0bde11bc4063683404022b
Dev address	0xc89c6cfd9d72cee7d1804b9d54b36b02d30e5038
Fee address	0xa7e1d822007f39686739c5445409807baa14927a
Procyon farming referral contract	0x464071a38d23de96e02aac9055ae9cbe0013f6bf

TOP 3 UNLOCKED WALLETS

1
N/A

2
N/A

3
N/A



FOUND THREATS

⚠ High Risk

Owner can change PCY tokens created (minted) for period of time without limitations.

```
function updateEmissionRate(uint256 _pcyPerBlock) public onlyOwner {  
    massUpdatePools();  
    emit EmissionRateUpdated(msg.sender, pcyPerBlock, _pcyPerBlock);  
    pcyPerBlock = _pcyPerBlock;  
}
```



FOUND THREATS

⚠ Medium Risk

Owner can change pool's last reward block which serve as time pointer for rewards minting and distribution.

```
function updateStartBlock(uint256 _startBlock) external onlyOwner {
    require(startBlock > block.number, "updateStartBlock: Farming already started");
    startBlock = _startBlock;

    uint256 length = poolInfo.length;
    for (uint256 pid = 0; pid < length; ++pid) {
        PoolInfo storage pool = poolInfo[pid];
        pool.lastRewardBlock = startBlock;
    }
}

function massUpdatePools() public {
    uint256 length = poolInfo.length;
    for (uint256 pid = 0; pid < length; ++pid) {
        updatePool(pid);
    }
}

function updatePool(uint256 _pid) public {
    PoolInfo storage pool = poolInfo[_pid];
    if (block.number <= pool.lastRewardBlock) {
        return;
    }
    uint256 lpSupply = pool.lpToken.balanceOf(address(this));
    if (lpSupply == 0 || pool.allocPoint == 0) {
        pool.lastRewardBlock = block.number;
        return;
    }
    uint256 multiplier = getMultiplier(pool.lastRewardBlock, block.number);
    uint256 pcyReward = multiplier.mul(pcyPerBlock).mul(pool.allocPoint).div(totalAllocPoint);
    pcy.mint(devAddress, pcyReward.div(10));
    pcy.mint(address(this), pcyReward);
    pool.accPCYPerShare = pool.accPCYPerShare.add(pcyReward.mul(1e12).div(lpSupply));
    pool.lastRewardBlock = block.number;
}
```



FOUND THREATS

Low Risk

Owner can edit existing pool's parameters such as rewards and fees.

```
function set(uint256 _pid, uint256 _allocPoint,
uint16 _depositFeeBP, bool _withUpdate) public onlyOwner {
    require(_depositFeeBP <= maxDepositFee,
        "set: invalid deposit fee basis points");
    if (_withUpdate) {
        massUpdatePools();
    }
    totalAllocPoint = totalAllocPoint.sub(poolInfo[_pid].allocPoint).add(_allocPoint);
    poolInfo[_pid].allocPoint = _allocPoint;
    poolInfo[_pid].depositFeeBP = _depositFeeBP;
}
```



Informational

Owner can add new pools and set desired parameters for them.

```
function add(uint256 _allocPoint, IBEP20 _lpToken,
uint16 _depositFeeBP, bool _withUpdate) public onlyOwner {
    require(_depositFeeBP <= maxDepositFee,
        "add: invalid deposit fee basis points");
    if (_withUpdate) {
        massUpdatePools();
    }
    uint256 lastRewardBlock = block.number > startBlock ? block.number : startBlock;
    totalAllocPoint = totalAllocPoint.add(_allocPoint);
    poolInfo.push(PoolInfo({
        lpToken: _lpToken,
        allocPoint: _allocPoint,
        lastRewardBlock: lastRewardBlock,
        accPCYPerShare: 0,
        depositFeeBP: _depositFeeBP
    }));
}
```

Owner can change referral contract address.

```
function setProcyonFarmingReferral(IProcyonFarmingReferral _procyonFarmingReferral)
public onlyOwner {
    procyonFarmingReferral = _procyonFarmingReferral;
}
```

Owner can change referral commission rate up to 4%.

```
uint16 public constant maxReferralCommissionRate = 400;

function setReferralCommissionRate(uint16 _referralCommissionRate) public onlyOwner {
    require(_referralCommissionRate <= maxReferralCommissionRate,
        "setReferralCommissionRate: invalid referral commission rate basis points");
    referralCommissionRate = _referralCommissionRate;
}
```




Informational

Owner can change dev address and fees address.

```
function setDevAddress(address _devAddress) public {
    require(msg.sender == devAddress, "setDevAddress: FORBIDDEN");
    require(_devAddress != address(0), "setDevAddress: ZERO");
    devAddress = _devAddress;
}

function setFeeAddress(address _feeAddress) public {
    require(msg.sender == feeAddress, "setFeeAddress: FORBIDDEN");
    require(_feeAddress != address(0), "setFeeAddress: ZERO");
    feeAddress = _feeAddress;
}
```

CONTRACT 3 INFO

Token Name
ProcyonFactory

Symbol
N/A

Contract Address
0x280bDa3B6E6846e011C5497F10bC984AaEA74a94

Network
Cronos Chain

Language
Solidity

Deployment Date
July 25, 2022

Verified?
Yes

Total Supply
N/A (Pair factory)

Status
Deployed

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



Informational

The contract is fork of PancakeSwap's Factory contract.

No threats found in this contract.



CONTRACT 4 INFO

Token Name
ProcyonRouter

Symbol
N/A

Contract Address

0x2117E09f5a8035332146718a899FFCdb3393fd3a

Network

Cronos Chain

Language

Solidity

Deployment Date

August 08, 2022

Verified?

Yes

Total Supply

N/A (Routing contract)

Status

Deployed

TAXES

Buy Tax
none

Sell Tax
none

*All routed transfers are subject to 0.3% tax



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



Informational

The contract is fork of PancakeSwap's Router contract.

No threats found in this contract.





RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Procyon

GOOD PRACTICES FOUND

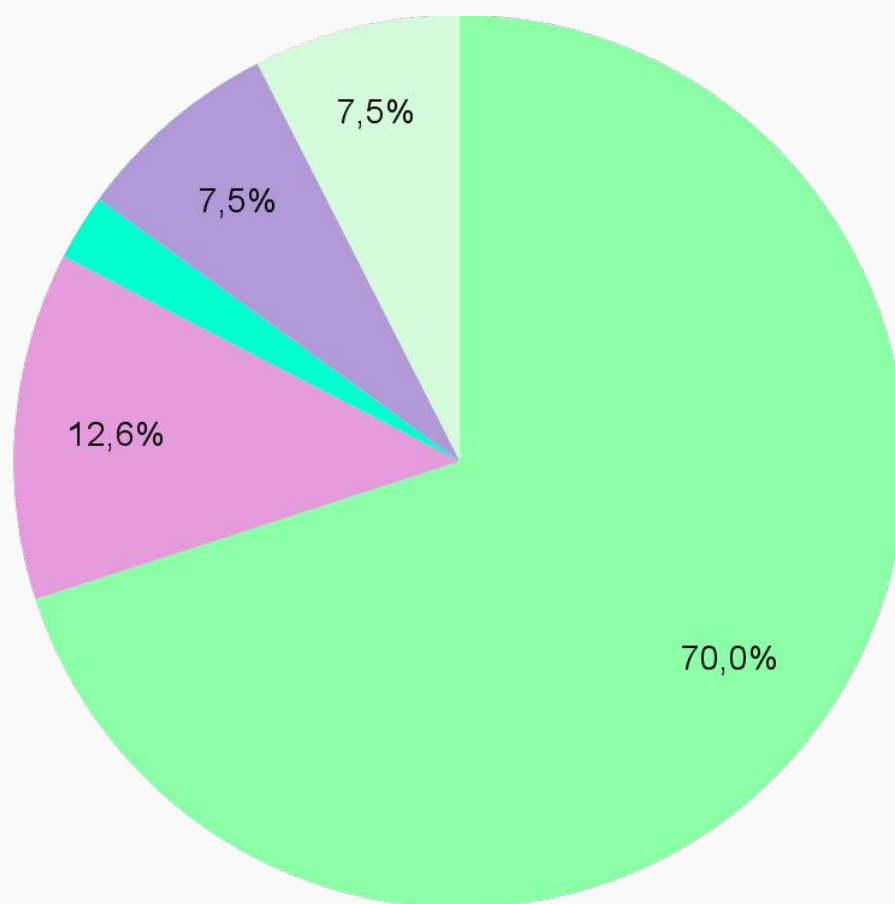
- ✓ The owner cannot stop or pause the contract
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



*The following tokenomics are based on the project's whitepaper and/or website:

- 70% - Seed round
- 12.6% - Liquidity
- 7.5% - Procyon team
- 7.5% - Marketing
- 2.4% - Viral campaign

- Presale
- Liquidity
- Viral campaign
- Team
- Marketing



TOKENOMICS



THE TEAM

! The team is
anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://procyon.finance>

Domain Registry

<https://www.namecheap.com>

Domain Expiration

Expires on 2023-06-15

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Appropriate color scheme and graphics.

Content

The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper

Well written, explanatory.

Roadmap

Yes, goals set with time frames.

Mobile-friendly?

Yes



procyon.finance



SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

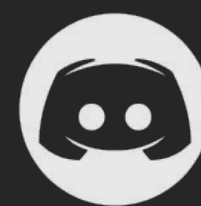
Project's social activity is
moderate with organic users



Twitter

@procyon_finance

- 624 followers
- 2 posts total made for month ⚠️



Discord

<https://discord.com/invite/jqQv9CjM3V>

- 18 members
- Active members



Telegram

@ProcyonFinance

- 116 members
- Active members
- Active mod



Medium

@ProcyonFinance

- 2 articles



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.